班级：2021 整合科学班　学号：2000012272　姓名：张广欣　评分：
同组学生：陈相如，倪丹
实验名称：量子加密

1　实验 8 量子加密

1. 实验原理

（1）光的偏振和量子通道

经典的现代通信体系基本建立在电磁波的基础上，目前该技术已经极为成熟。

1865 年麦克斯韦方程组被提出后，人们对电磁波的认识达到了相当深入的水平。在爱因斯坦和普朗克提出的光量子理论被验证后，人们知道了电磁波是由光子组成的。日常传输信息时所用的电磁波都是由巨量光子组成的，比如 4G 手机接收到的 1bit 信息都是由超过 100 万个光子携带，因此经典通信的信号稳定，不容易被噪声干扰且有很成熟的纠错编码方法（汉明码等）；且目前人们可以通过调整电磁波的频率来传递，这样就和光的偏振方向无关，在传输过程中，光的偏振状态很难改变，强度可以通过中继放大器补偿。而对于量子通道，其稳定性远远不如经典信道，因此目前的量子通信只是用来远距离传输密钥。

在量子通信领域，人们几乎都是用光子来携带比特信息的，主要原因是：

（1）光在通常环境中量子效应仍然显著。

（2）经典信道中人们已经积累了很多光通信的技术。

量子通信将信息编码到光子的偏振态中，再将编码后的光字通过量子信道传输到远方，从这个角度上看，量子通信和经典通信可传输的信息并无不同。由于传输的信号是以单个光子为单位，很容易受到噪音干扰，量子信道对信道的要求极高，且并不能避免信号随距离的衰减，因此需要量子中继来补充光子，但又被量子的不可克隆性所限制，这一困难至今没有被完全克服，极大影响了量子通信的应用。

规定光子的水平偏振态为 $|0\rangle$，垂直偏振态为 $|1\rangle$，其他偏振态可视为 $\alpha|0\rangle+\beta|1\rangle$。

以某一方向的方解石状态为例：已知偏振态的光子从左边入射，如果偏振方向为水平 $|0\rangle$，那么将不受影响。如果偏振方向垂直 $|1\rangle$，光子将向下平移，从右侧射出后仍然保持原来的偏振状态。如果偏振态为 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$，那么该光子通过方解石后有 $|\alpha|^2=|<\psi|0>|^2$ 的概率变成水平偏振，$|\beta|^2=|<\psi|1>|^2$ 变成垂直偏振并向下发生偏移。

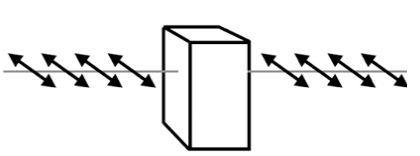

图 1: 偏振方向为水平

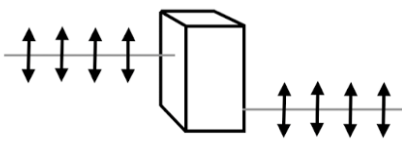

图 2: 偏振方向垂直

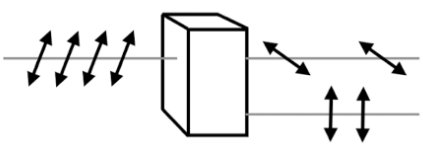

图 3: $\alpha|0\rangle+\beta|0\rangle$

如果旋转这块方解石与垂直方向偏离 45 度，这时可以不受影响穿过方解石的偏振态为 $|0_x\rangle=$

$(|0\rangle + |1\rangle)/\sqrt{2}$; 而偏振态 $|1_x\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ 的光子通过此状态的方解石后会保持自己的偏振态。因此称 $|0_x\rangle$ 为 45 度角偏振态，把 $|1_x\rangle$ 称为 135 度角偏振态。本实验采用的方案就是将方解石旋转到偏离垂直方向 45 度。

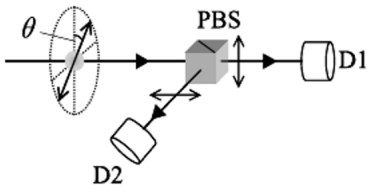

图 4: 单光子被调制到指定偏振角度，接收端通过一个偏振分波器将光子分束到 D1 或 D2 任一探测器

（2）半玻片

波片，又称相位延迟片，它是由双折射的材料加工而成。用于调整光束的偏振状态。常见的波片由单轴晶体（如石英晶体）制作而成，其表面与光轴平行，垂直于光轴的偏振分量（o 光）与平行于光轴的偏振分量（e 光）在晶体中不发生双折射，但传播速度不同，因而通过波片后它们仍然沿着原有的方向传播，且会产生相位偏移。

偏振光通过半波片后，仍为线偏振光，但是，其合振动的振动面与入射线偏振光的振动面转过 2θ。若 $\theta = 45°$，则出射光的振动面与原入射光的振动面垂直，也就是说，当 $\theta = 45°$ 时，半波片可以使偏振态旋转 90°。

（3）BB84 协议

1984 年，Charles Henry Bennet 和 Gilles Brassard 首次提出以量子力学原理产生密码的方案，被称为 BB84。之后的各种量子加密方案（B92 等）与其基本流程相似：Alice 和 Bob 使用量子信道，与经典信道配合产生密钥，之后使用经典信道进行加密通信。

BB84 方案的流程：

（1）Alice 随机产生 2 组等长的随机二进制数字 a, b，一组确定选用的基，另一组为发送的比特。

（2）Alice 以每对数字 a_k, b_k 向 Bob 发送一系列偏振态 $|\psi_{a_k b_k}\rangle$ 规则为：

$|\psi_{00}\rangle = |0\rangle$

$|\psi_{10}\rangle = |1\rangle$

$|\psi_{01}\rangle = |0_x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$

$|\psi_{11}\rangle = |1_x\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

（3）Bob 随机产生一列二进制数 b‘$_k$ 并根据其以相似的方式来确定以何种偏振态来接收 Alice 发来的偏振光子，得到的结果以另一列二进制数 b’ 表示。

（4）Alcie 公布 b，Bob 将其和 b' 逐位比较，如果 $b_k = b'_k$，则保留 $a\ k$；如果 $b_k = b'_k$，则放弃 a'_k。鲍勃通过经典信道告诉爱丽丝在哪些位数 k 上，$b_k = b'k$，并公布部分 $b'k$ 对应 $a'k$ 的测量值，若与 Alice 发送的 b_k 相同，则确认此信道没有受到监听，$a'k$ 的其余部分则作为密钥。为了安全和抗干扰，一般情况下，如果想得到一个 n 位的二进制密码 a, b 会被选成具有 $4n + \delta$ 位的二进制数，比较 δ 大，根据具体实际情况来确定。Alice 和 Bob 会从保留下的大约 2n 个 a_k 或 a'_k 中再随机选

出 n 个，在经典信道中相比较，如果符合率很高，就保留没有公开的 a_k 和 a'_k; 如果符合率很差，就重新开始。

在得到密钥后，Alice 便可以将所要所要传输的信息转化为二进制，然后通过与密钥进行异或运算得到密闻，然后从经典信道给 Bob 传输密文即可。

2. 实验过程

分工：Alice：张广欣 Bob：倪丹 Eve：陈相如

（1）组装 Thorlab 的教学套件

之后的实验过程与实验原理中提到的基本相同。

（2）Alice 以保密的偏振方式通过“量子信道”向 Bob 传输 52bit 信息，Bob 以随机方式接收。

（3）Bob 公布自己接收偏振光的方式，Alice 告诉 Bob 在哪些位数上，二者信息的收发方式相同。Bob 公布部分两者接收方式相同位数上自己的观测数据供 Alice 核对（与实验原理中提到的方法略有不同，但二者等价），若公布的部分二者相同，这判定没有被偷听，二者相同偏振方式没有被公布的字符串作为密钥。反之则宣布失败，重新开始。

（4）得到密钥后，Alice 将想要传输的信息转化成二进制字符串，与密钥取异或运算得到密文，通过任何一种经典信道告诉 Bob 密文，本实验中采用直接告知。

（5）Alice 和 Bob 中加入偷听的 Eve，Eve 在 Alice 传输信息时以随机偏振方式接收光子，并将此结果以完全相同的方式发送给 Bob。Bob 用上文提到的方案得知自己被偷听。

3. 实验结果

1.Alice 给 Bob 发送一系列偏振光子，Bob 随意接收（此过程发生在量子信道）

Alice	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis(+ or x)	+	x	+	+	x	x	+	+	+	+	+	x	x	+	+	+	+	+
Bit(0 or 1)	0	1	0	1	1	0	1	0	0	0	0	0	1	1	1	0	0	1
	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis(+ or x)	x	x	x	x	+	+	+	+	+	+	+	x	x	x	x	x	+	+
Bit(0 or 1)	1	1	0	0	0	1	0	1	1	0	1	0	0	0	0	1	0	1
	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
Basis(+ or x)	x	+	+	+	+	+	+	+	+	x	x	x	+	+	+	+		
Bit(0 or 1)	1	1	0	1	0	0	1	1	1	0	1	1	1	1	0	1		
Bob	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis(+ or x)	+	x	+	+	x	+	x	+	x	+	x	x	+	x	+	+	x	x
Bit(0 or 1)	0	0	1	1	1	0	1	0	1	1	0	0	0	1	1	0	1	0
	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis(+ or x)	+	x	x	x	+	+	x	+	+	x	x	+	x	+	+	x	x	x
Bit(0 or 1)	1	1	0	0	1	1	0	1	1	1	1	1	0	0	0	1	1	0
	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
Basis(+ or x)	+	x	x	+	+	x	x	+	+	+	x	+	x	x	+	+		
Bit(0 or 1)	1	0	1	1	0	0	1	1	1	0	1	0	1	1	1	1		

2.Bob 告诉 Ailce 自己所有的基，Alice 告诉 Bob 两者一样的基的位数，Bob 给 Ailice 发送部

分结果作为校验（此过程发生在经典信道）

相同基的序号	1	2	3	4	5	8	10	12	15	16	20	21	22	23	24	26	27	31
bit（0 or 1）	0	1	0	1	1	0	0	0	1	0	1	0	0	0	1	1	1	0
相同基的序号	34	40	41	44	45	47	51	52										
bit（0 or 1）	1	1	0	1	1	1	0	1										
校验位数	1	3	20	26	41	51												
检验码	0	0	1	1	0	0												
密码位数	2	4	5	8	10	12	15	16	21	22	23	24	27	31	34	40	44	45
密钥	1	1	1	0	0	0	1	0	0	0	0	1	1	0	1	1	1	1
密码位数	47	52																
密钥	1	1																

3.Alice 将信息转化为二进制后与密钥进行亦或运算得到密文，密文直接通过经典信道传输（不再需要量子信道）。Bob 直接对密文与密钥进行异或运算，得到信息。

发送的信息	F					A					D				
Representation	0	0	1	0	1	0	0	0	0	0	0	0	0	1	1
密钥	1	1	1	0	0	0	1	0	0	0	0	1	1	0	1
密文	1	1	0	0	1	0	1	0	0	0	0	1	1	1	0
发送的信息	E														
Representation	0	0	1	0	0										
密钥	1	1	1	1	1										
密文	1	1	0	1	1										

4. 有 EVE 存在时，重复密钥分发的方案

Alice	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis(+ or x)	+	+	+	x	x	+	+	x	+	+	+	x	x	x	+	+	+	x
Bit(0 or 1)	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0
	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis(+ or x)	x	+	+	x	+	+	+	+	+	x	x	+	+	x	x	x	+	+
Bit(0 or 1)	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1
	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
Basis(+ or x)	x	x	x	+	+	+	x	x	x	+	+	+	x	x	x	+		
Bit(0 or 1)	1	1	1	0	0	0	0	0	1	1	1	1	1	0	0	0		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	x	x	+	+	+	x	+	x	x	x	+	+	x	+	x	x	x	+
	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
EVE 使用的基																		

	+	+	+	+	x	+	x	x	+	+	x	+	x	x	x	+	+	x
	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
	+	x	+	+	+	+	x	+	x	x	+	+	x	+	+	+		
Bob	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis(+ or x)	+	+	x	+	x	+	+	x	x	x	+	+	+	+	x	x	+	x
Bit(0 or 1)	0	0	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0
	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis(+ or x)	+	x	+	+	x	x	+	x	x	x	x	+	+	+	+	x	+	x
Bit(0 or 1)	1	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	1	0
	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
Basis(+ or x)	+	x	x	+	+	+	x	x	x	x	+	+	+	+	x	+		
Bit(0 or 1)	1	1	0	0	0	0	1	1	1	0	1	1	1	1	1	0		

5. Bob 告诉 Ailce 自己所有的基，Alice 告诉 Bob 两者一样的基的位数，Bob 给 Ailice 发送部分结果作为校验（此过程发生在经典信道），发现错误，本轮通信终止。

如果选中标红的数据进行校验，会发现这一问题，但如果没有选中可能会没有发现 Eve 的存在。真实情况中可以通过加长密钥生成序列让这种可能趋于零。

Alice、Bob 选取的基相同	1	2	5	6	7	8	11	17	18	21	25	28	29	30	31	34	35
Basis(+ or x)	+	+	x	+	+	x	+	+	x	+	+	x	x	+	+	x	+
Alice 发送的 Bits	0	0	1	1	1	1	0	0	0	1	1	0	0	0	0	1	1
Basis(+ or x)	+	+	x	+	+	x	+	+	x	+	+	x	x	+	+	x	+
Alice 接收的 Bits	0	0	1	1	0	0	0	0	0	1	1	1	0	0	0	0	1
Alice、Bob 选取的基相同	39	40	41	42	43	44	45	47	48	51	52						
Basis(+ or x)	x	+	+	+	x	x	x	+	+	x	+						
Alice 发送的 Bits	1	0	0	0	0	0	1	1	1	0	0						
Basis(+ or x)	x	+	+	+	x	x	x	+	+	x	+						
Alice 接收的 Bits	0	0	0	0	1	1	1	1	1	1	0						

4. 本次实验的局限性

实际上，本次所用仪器仅为教学演示实验用，与真实的量子信道相距甚远

（1）真实的量子信道中，传输的信息单位是单光子，本次单次触发便传输了右眼可见的巨量光子，完全可以被监听而不被发现。

（2）本次对被监听的判断为 Alice 和 Bob 公布的接收方式的相通的比特位上有不同的比特即判定为被窃听。实际上任何信道都存在噪音，信号也有衰减的问题，应对设计好的信道反复进行大量测试，得到一个稳定的错误比例，二者核对信息时超过此比例才判定被窃听或通过更复杂的方式。

（3）本次传输信号的比特数过小，在信息论中，信道传输信息的性质应在“反复无限次传输”后才能较好确定，基于如此小样本的数据进行概率分析意义不大。

参考文献

[1] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
[2]Bennett, Charles H.; Brassard, Gilles (2014-12-04). "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science. Theoretical Aspects of Quantum Cryptography –celebrating 30 years of BB84. 560, Part 1: 7–11.
[3] 吴飚. 简明量子力学 [M]. 1. 北京大学出版社, 2020.